(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) Int. Cl.[6]
G09C 5/00

(45) 공고일자 1999년06월01일
(11) 등록번호 10-0187876
(24) 등록일자 1999년01월08일

(21) 출원번호 10-1996-0062291
(22) 출원일자 1996년12월06일
(65) 공개번호 특1997-0067054
(43) 공개일자 1997년10월13일

(30) 우선권주장 8/625,475
1996년03월29일
미국(US)

(73) 특허권자 인터내셔널 비지네스 머신즈 코포레이션 제프리 엘.포맨
미국 10504 뉴욕주 아몬크 뉴오챠드 로드

(72) 발명자 아우어바크 조슈아 세쓰
미국 06877 코네티컷주 리지필드 홈메스 로드 129

초 치-셍
미국 95014 캘리포니아주 쿠퍼티노 에이그스 레인 19030

카플란 마크 아담
미국 10536 뉴욕주 카토나 홈리 힐 레인 14

크리글러 제프리 찰스
미국 버지니아주 액린 딕시 플레이스 8601

(74) 대리인 장수길, 김성택

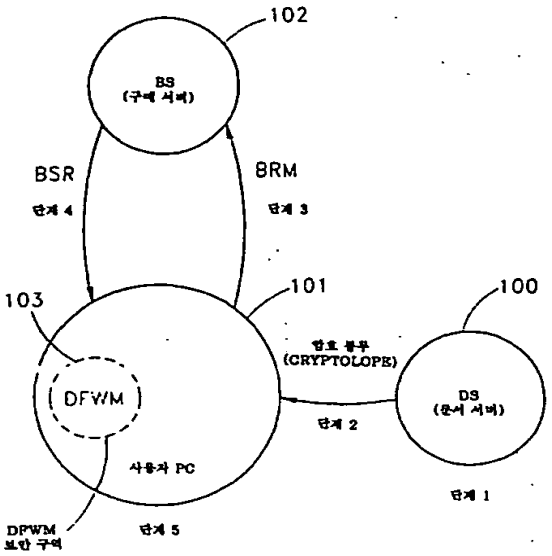
심사관 : 정성창

(54) 암호 봉투의 작성 및 배포 방법

요약

보안 유지 가능한 암호 봉투를 사용하여 디지털 문서의 작성, 배포, 판매 및 제어 접속을 하기 위한 장치 및 방법이 기재되어 있다. 봉투는 정보 부분들의 집단이며, 보호되는 이 각각의 부분들은 해당하는 부분 암호화 키에 의해 암호화된다. 이 암호화된 정보 부분들은 기타의 정보 부분들과 함께 봉투의 일부가 된다. 각각의 부분 암호화 키도 공개 키에 의해 암호화되는데, 이 암호화된 부분 암호화 키도 봉투 내에 포함된다. 봉투는 부분들의 목록을 또한 포함하는데, 이 목록의 각 항목은 부분 이름과 그 이름의 부분에 대한 보안 해시를 가진다. 이어서, 목록은 비밀키에 의해 서명되어 서명을 발생시키는데, 이 서명도 봉투에 포함된다. 서명은 제1도 비밀 키에 관련된 제2도 공개 키를 사용하여 조회될 수 있으며, 봉투 내의 임의의 정보 부분의 보존은 제2도 해시를 계산하고 그 결과를 부분들의 목록의 해당하는 해시와 비교함으로써 검사될 수 있다. 또한, 임의의 암호화된 부분들의 정보 내용은 부분 암호화 키들을 암호화하는데 사용된 공개 키에 해당하는 제2도 비밀 키를 알아야만 복구될 수 있다

대표도



명세서

도면의 간단한 설명

제1도는 암호 봉투 처리의 5단계를 계략적으로 도시한 도면, 본 처리에 관계된 주요 요소는 문서 서버(DS, 100), 구매 서버(BS, 102), 해독 지문과 워터마크처리 모듈(DFWM : decryption fingerpinting and watermarking module, 103), 및 사용자 개인용 컴퓨터(UPC, 101)이다.

제2도는 전형적인 암호 봉투의 구조를 도시한 도면. 최소한의 요소는 암호화된 부분(203)과 이에 관련된 암호화된 부분 암호화 키(PEK : part encryption key, 202), 부분들의 목록(list of parts, 209), 및 부분들의 목록의 서명(208)이다.

제3도는 부분들의 목록(209)을 가지는 BOM(bill of materials, 자료 명세표)의 구조를 도시한 도면. 이 표의 각 항목은 예컨대 초록과 같은 부분 이름(302), 및 예컨대 13ADBF77F...와 같은 그 이름을 가진 부분의 보안 해시(secure hash)인 MessageDigest5(MD5)를 포함한다. 목록의 MD5이 계산되고 그 해시 결과가 DS의 비밀 키를 사용하여 서명되어 디지털 서명(208)을 발생한다.

제4도는 전형적인 가격 행렬(price matrix)을 도시한 도면. 열(columns)은 여러 가지 회원 유형(membership categories, 402, 403, 404, 405)에 대한 할인율을 나타내며, 행(rows)은 구매량에 따른 할인(quantity discount, 406, 407, 408, 409)을 나타낸다. n번째 사본에 대한 가격과 n개의 사본에 대한 총 가격을 계산하기 위한 공식의 예가 (401)로 나타나 있다.

제5도는 구매 요청 메시지(BRM : Buy Request Message, 500)을 도시한 도면. BRM에는 암호화된 PEK(202, 211), 암호화된 지문과 워터마크 처리 명령(205), 기간과 조건(206), 및 BOM(207)이 포함된다. 항목(202, 205, 206, 207 및 211)은 암호 봉투(200)로부터 복사된다 (제2도 참조). BRM의 기타 부분들(501 내지 505)은 UPC에서 발생된다.

제6도는 구매 서버 응답(BSR : Buy Server Response, 600)이다. 구매 서버(BS)는 PEK를 번역하여 DFWM(103)만이 해독할 수 있는 번역된 PEK(602, 603)을 발생한다. 지문과 워터마크 처리 명령은 해독되고, 커스텀화되며(customized), 재암호화되고, 결과(604)는 DFWM에 의해서만 해독될 수 있다. BRM(500, 5도)의 기간과 조건은 또한 평가되며 갱신되거나 변환된 기간과 조건(605)를 발생할 수 있다. 실제의 구입 가격(601)은 기본 가격에 적절한 할인을 하여 계산된다.

* 도면의 주요부분에 대한 부호의 설명

100 : 문서 서버(DS)　　101 : 사용자 PC

102 : 구매 서버(BS)　　103 : 해독 지문과 워터마크 처리 모듈(DFWM)

200 : 암호 봉투　　207 : 자료 명세표(BOM)

400 : 가격 행렬　　500 : 구매 요청 메시지(BRM)

600 : 구매 서버 응답(BSR)

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 보안 유지 가능한 암호 봉투 방법과 기법을 사용하여 디지털 문서의 작성, 배포 및 판매, 그리고 통제 하의 접속을 하기 위한 방법(s method for creation, distribution, and sale and for the controlled

access of digital documents using the methods and techniques of secure cryptographic envelopes)에 관한 것이다.

디지털 문서는 종이로 된 아날로그 문서에 비해 많은 장점을 가진다. 디지털 문서는 작성, 배포 및 복사하기가 용이하다. 그러나, 이러한 장점들은 디지털 문서에 관련된 지적 소유권을 침해자로부터 보호하는 것을 어렵게 만들기도 한다. 그럼에도 불구하고, 디지털 문서는 향후 정보의 배포 및 판매를 위한 매개체로서 종이 문서를 대체할 것이다.

[CD 쇼케이스(CD-Showcase, 미국특허 제5, 319, 705호)]

본 발명과 CD 쇼케이스 특허[2] 사이의 중요한 차이는 본 발명에서는 부분 암호화 키(part encryption key)가 암호 봉투 내에 실리며 공개 키(public key)에 의해 암호화된다는 점이다. 반면에 CD 쇼케이스 특허에서는, 배포된 데이터에 암호화 키의 식별자(identifier of the encryption key) 만이 포함된다. 암호화 키는 서버(server)에 저장되며 키 식별자의 제시에 의해 얻어진다.

따라서, CD 쇼케이스 특허의 경우, 서버가 키 데이터베이스를 운용할 필요가 있으며, 이 때문에 구매 서버(buy server)와 문서 서버(document server) 사이의 신뢰도의 파악이 필요하게 된다.

[PGP(Pretty Good Privacy,.프리티 굿 프라이버시)]

PGP[3]은 보안이 된 전자 우편(e-mail)을 보내기 위한 공개 키 개념에 기초한 시스템이다. 전자 우편의 본문은 IDEA 알고리즘을 사용하여 암호화되며 (예컨대 [1] 참조), 암호화 키는 목적하는 수취인의 공개 키를 사용하여 암호화된다. 수취인은 자신의 비밀 키(secret key)를 사용하여 암호화 키를 복원하며, 이어서 이 복원된 암호화 키를 사용하여 보통의 텍스트(plain text)를 복원한다.

발명이 이루고자하는 기술적 과제

본 발명은 보안 유지 가능한 암호 봉투(secure cryptographic envelopes) 방법과 기법을 사용하여 디지털 정보의 작성, 배포, 및 판매를 하기 위한 방법에 관한 것이다. 암호 봉투는 무단의 판독 및 변경(unauthorized reading and tampering)으로부터 문서 부분(document parts)의 보안을 유지하기 위하여 이를테면 암호화(encryption) 및 인증(authentication)과 같은 현대적인 암호 기법(cryptographic echniques)을 사용한다.

본 발명의 처리에 따르면 사용자가 암호 봉투의 부분들을 구입할 수 있으며, 그 정보 내용은 보안이 유지되며 통제가능한 방식으로 방출된다. 해적 행위(piracy)를 방지하기 위해 그 부분들에 대하여 추가적인 처리가 행해진다. 또한, 공개 키 기술의 사용에 의하여 암호 봉투 기법은 디지털 정보를 배포하는 편리하고, 안전하며, 일체 완비(self-contained)된 수단이 된다.

[슈퍼 디스트리뷰션(Super distribution)]

본 명세서에서는 정보 배포의 기초 모델로서 슈퍼 디스트리뷰션을 가정한다(보다 구체적인 설명은 [5] 참조). 기본적인 아이디어는 각각의 문서들이 암호화되기만 한다면, 디지털 문서(또는 부분들)이 라디오 또는 텔레비젼 신호, 케이블, 위성, LAN(Local Area networks, 근거리 통신망), 디스켓, CD-ROM, 및 BBS에 의해 인터넷 상에서 자유롭게 배포될 수 있다는 것이다. 암호화 처리가 보안을 충분히 유지시킨다고 가정하면, 사용자가 그 내용에 접속할 수 있는 유일한 방법은 필요한 PEK(part encryption keys)를 구입하는 것 뿐이다. 여기서 PEK는 전형적으로는 해독(decrypt)하는 문서보다 그 크기가 더 작다.

슈퍼 디스트리뷰션은 정보 배포의 문제를 (1) 대량의 데이터(bulk data) 배포와 (2) PEK 배포를 통한 내용의 통제된 배포로 분리해 주므로 중요한 개념이다.

본 발명은 이 기본 개념을 확장하며, 내용 배포와 판매를 위하여 암호 봉투라는 기법을 도입한다. 또한, 이 개념과 기법은 디지털 문서의 접속과 사용에 대한 임의의 기간과 조건도 취급할 수 있도록 일반화된다. 이 일반화에 의하여, 디지털 문서의 분산 접속 제어의 설계와 구현을 위한 기초로서(as a basis for designing and implementing distributed access control of digital documents) 암호 봉투를 사용할 수 있게 된다.

본 발명에 따르면, 서버가 키 데이터베이스를 운용할 필요가 없게 되며, 또한 문서 서버(Document Server, 내용물이 암호화되는 장소)와 구매 서버(Buy Server, 문서 암호화 키를 얻을 수 있는 장소) 사이의 신뢰관계를 보다 명백히 분리할 수 있게 된다.

따라서, 허가된 사용자만이 보안 정보 부분의 깨끗한 텍스트 내용(the clear text content of the secure information parts)에 접근할 수 있으며, 임의의 수의 사용자에게 임의로 배포될 수 있는 암호 봉투의 작성 방법을 제공한다. 본 발명에 의하면, 각각의 정보 부분들은 해당하는 부분 암호화 키에 의해 암호화되어 암호화된 정보 부분을 발생한다. 이어서 각 부분 암호화 키는 공개 키에 의해 암호화된다. 봉투에 포함되는 부분들의 목록도 생성되며, 목록의 각 항목은 부분 이름과 그 이름을 가진 부분으 보안 해시(secure hash of the named part)를 가진다. 이어서, 봉투는 암호화된 정보 부분, 암호화되지 않은 정보 부분, 암호화된 부분 암호화 키와 부분들의 목록을 포함한다. 마지막으로, 부분들의 목록은 비밀 키에 의해 서명되어 서명을 발생하며, 이 서명도 봉투에 포함된다. 목록의 보존(integrity of the list)은 목록에 서명하는데 사용된 비밀 키와 관계된 제2 공개 키를 사용하여 검사될 수 있다. 임의의 어느 한 정보 부분의 보존은 그 부분에 제2 해시를 계산하고 제2의 해시를 그 목록의 부분에 대한 해당 해시와 비교함으로써 검사될 수 있다. 마지막으로 암호화된 부분의 정보 내용의 공개가 방지될 수 있고 부분 암호화 키에 의해서만 복원될 수 있으며, 암호화되지 않은 부분 암호화 키를 얻기 위해서는 공개 키에 해당하는 비밀을 알고 있어야 한다. 그 후 나중의 암호화되지 않은 키를 사용하여 정보 부분으로부터 보통의 텍스트를 발생한다.

발명의 구성 및 작용

제1도를 참조하면, 암호 봉투 처리의 중요한 장점중의 하나는 보안(security)이다. BS(구매 서버, 102)와 DS(문서 서버, 100)은 보안이 유지된다고 가정한다. 예를 들어, BS와 DS는 기업의 각 업무 파트너에 의해 소유되어 관리되며, 신뢰할 수 있는 직원에 의해 유리 방(glass house)에서 운영되고 있다.

또한, UPC(사용자 개인용 컴퓨터, 101)는 사용자에게 속하기 때문에, 비교적 작으며 보안 유지 가능한 DFWM(Decryption Fingerprinting and Watermarking Module, 해독 지문과 워터마크 처리 모듈, 103) -

DFWM에서는 소프트웨어 또는 무단 변경 방지 하드웨어(tamper-resistant hardware)를 통해 보안이 유지된다 - 을 제외하고는, UPC에서는 보안이 그다지 잘 유지되지 않는다고 가정한다.

[처리 단계의 개괄]

처리 단계의 개괄은 다음과 같다 (제1도 참조).

단계 1 암호 봉투 작성(Cryptographic Envelope Creation)

단계 2 암호 봉투 배포(Cryptographic Envelope Distribution)

단계 3 사용자의 구매 요청(User-Initiated Buy Request)

단계 4 구매 서버 응답(Buy Server Response)

단계 5 암호 봉투의 개봉(Opening of Cryptographic Envelope)

[암호 봉투의 처리 단계]

각각의 처리 단계들을 더욱 상세히 설명한다.

[단계 1 : 암호 봉투 작성]

첫 단계는 암호 봉투의 작성이다. 제2도의 (200)을 참조한다. 디지털 문서들의 모음을 슈퍼 디스트리뷰트하는 것이 필요할 것이므로 암호 봉투의 작성은 내용 제공자가 보통 오프라인(off-line)으로 행한다.

선택적으로, 사용자의 요청에 의하여 암호 봉투의 작성이 개시될 수 있다. 이 경우, 암호 봉투가 그 사용자를 위해 특별히 작성되며, 그 사용자 또는 요청에 따른 특정한 소정의 정보가 암호 봉투에 포함될 수 있다. 또한, 나중에 다른 사용자로부터 비슷한 요청이 있을 것이 예상되는 경우, 추가적인 정보를 암호 봉투에 포함시킬 수 있으며, 이 암호 봉투는 미래에 비슷한 요청이 보다 효율적으로 수행될 수 있도록 하기 위해 저장된다(cashed).

[암호 봉투 부분(Cryptographic Envelope Parts)]

암호 봉투는 정보 부분들의 집단(a grouping of information parts)이다. 제2도의 (210 내지 211)을 참조하라. 이 정보 부분들 중의 일부는 암호화되며, 나머지 부분들은 깨끗한 텍스트(clear text)로 있다. 암호 봉투 처리는 다양한 군집화 기술 (grouping technologies, 예를 들어, zip, tar, 및 OpenDoc Bento와 Microsoft OLE의 보다 객체 지향적인 접근 방식)과 호환가능하다. 군집화 방법에 대한 요구사항은 최소한 다음과 같다. 즉, (1) 부분들이 배포하기에 적합한 단위로 모일 수 있으며, 그 부분들이 나중에 각자 복원될 수 있을 것과, (2) 이를테면 이름붙이기(naming), 포인터, 및 색인과 같이 서로 다른 부분들을 관련시키는 수단이 있을 것이다.

정보 부분들은 문서형(document, 201 및 203)과 제어형(control, 202, 204 내지 211)의 두가지 유형이 있다. 문서 부분들은 내용(contents)이다. 문서 부분들의 예로는 초록, 목차, 도면, 표, 및 텍스트가 있다. 문서 부분들은 실행가능한 프로그램, 서브루틴들의 라이브러리, 소프트웨어 모듈 또는 객체 요소의 일부분(portions of an executable program, a library of subroutines, software modules, or object components)일 수도 있다.

제2도를 참조하면, 문서 부분은 암호화될 수 있다(203). 암호화된 문서 부분(203)은 사용자에 의해 구매될 중요 가치있는 내용(valuable contents)이다 (예컨대, 책의 한 섹션, 고해상도 JPEG 화상, 또는 MPEG 스트림). 암호화되지 않은 부분은 맛보기 부분(teasers, 201)이다 (예컨대, 타인에 의한 책의 리뷰, 목차, 초록, 또는 저해상도 JPEG 화상). 암호화되지 않은 부분의 목적은 사용자가 실제로 구매하기 전에 암호 봉투의 내용을 프리뷰(preview)하거나, 표본(sample)을 보거나, 훑어(browse)볼 수 있도록 해주는 것이다.

압축과 특별한 스트링 패턴의 삽입(compression and insertion of special string patterns)과 같은 전처리(preprocessing)를 문서 부분에 적용할 수 있다. 압축은 저장기를 감소시킨다. 기타의 전처리는 DFWM이 문서 부분들에 지문과 워터마크 처리를 할 수 있도록 문서 부분을 수정하는 것이다.

제어 부분은 암호 봉투의 기능 및 처리 모델을 지원하기 위해 필요한 메타데이타이다. 여기에는 인증(anthenticity)과 비밀 유지(confidentiality)라는 두가지 주요 기능이 있다. 암호 봉투의 내용은 무단으로 변경되지 않느다(not tampered). 인증 기능은 디지털 서명을 사용하여 이루어진다. 비밀 유지 기능은 암호화에 의해(예컨대, DES 또는 IDEA를 사용하여) 이루어진다. 이 암호화와 인증 기법의 기초는 당업계에서 공지되어 있으며, 암호학에 관한 임의의 현대 교과서 (예컨대, [1] 참조)에서 찾아볼 수 있다. 모든 제어 부분은 인증되며 그 중 일부는 필요한 경우 암호화될 수 있다.

제어 부분의 예로는 가격 행렬(price matrix, 제4도의 400 참조) 및 문서 부분의 후처리(post-processing)를 위한 지문과 워터마크 처리 명령(205)이 있다. 문서 부분의 후처리는 암호 봉투가 개봉될 때, DFWM에 의해 수행된다. 지문과 워터마크 처리는 후처리의 예이며, 해적 행위를 방지하도록 문서 부분에 표식을 한다(mark document parts in a way to deter piracy).

제4도를 참조하면, 가격 행렬(400)은 예컨대 여러개의 사본을 구입하는데 대한 구매량 할인(volume discount), 클럽 회원 할인(discount for club membership), 협력사 할인(corporate discount)과 같이 문서 부분의 구입에 대한 가격 구조를 기술한다. 문서의 사본 n개의 구매 가격을 계산하기 위한 예시적인 공식(401)이 도시되어 있다. (가격 할인율은 시기에 따라 달라질 수도 있으며, 이 경우 가격 행렬의 열(402 내지 405)는 클럽 회원 대신에 제한된 기간의 특별 제공가일 수 있다는 점에 주목하여야 한다).

제2도를 참조하면, 문서 부분의 구입과 사용에 대한 기간과 조건(206)도 암호 봉투 내에 포함될 수 있다. 이들은 문서 부분으로서 포함될 수 있으며 (이 경우 사용자가 볼 수 있게 된다) 또는 제어 부분으로서 포함될 수 있다 (이 경우 구매 서버(BS, 102)에서 그리고 다시 사용자의 개인용 컴퓨터(UPC, 101)에서 이 기간과 조건을 평가한다). 문서 부분은 텍스트로된 정보를 포함하며, 제어 부분은 기간과 조건을 구현하는 프로그램 (예컨대, Per[4]와 같은 스크립팅 언어(scripting language)로 작성된다)을 포함할 수 있다 (지문과 워터마크 처리 명령, 및 가격 행렬을 주목한다. 명확을 기하기 위해 이들을 나열하였다).

[비밀 유지 및 인증Confidentiality and Authenticity)]

이제 비밀 유지가 어떻게 이루어지는지 그 방법을 기술한다. 가치 있는 부분들은 DES(Data Encryption

Standard, 데이터 암호화 표준) 알고리즘 ([1] 참조)을 사용하여 암호화된다. 서로 다른 부분들은 서로 다른 PEK(part encryption keys, 부분 암호화 키)를 사용하여 암호화한다. 이들 키는 무작위로 독립적으로 선택된다.

불규칙 암호화 키(random encryption key)를 발생하는 방법은 많이 있다. 그 한 방법은 불규칙 스트링(randon string)을 만들기 위해 불규칙 또는 의사 불규칙 수 발생기(random or pseudo-random number generator)를 사용하는 것인데, 이 불규칙 스트링이 키로서 사용된다. 이 방식에 관한 보다 상세한 사항은 [1, 3]에서 찾아볼 수 있다.

각 PEK는 BS(102)의 공개 키를 사용하여 암호화되며, 암호화된 PEK(202, 제2도) 결과는 암호 봉투의 제어 부분이 된다. (PEK는 서로 다른 BS 공개 키를 사용하여 암호화될 수 있으며, 이 암호화된 모든 PEK는 암호 봉투 내에 포함된다는 점에 주목한다.)

암호 봉투와 그 부분들에 대한 인증을 보장하기 위한 여러 가지 방법들이 있다. 이러한 방법 중의 하나를 이제 설명한다. 모든 암호 봉투는 BOM(Bill of Materials, 207)이라는 특별한 제어 부분을 가진다. BOM은 (1) 부분들 목록(209), 및 디지털 서명(208)의 두 개의 부분으로 이루어진다.

보안 해시 기능(secure hash function), MessageDigest5(MD5)을 암호 봉투에 포함된 각 부분에 적용하여 (상세한 사항은 예컨대 [1] 참조), 목록을 작성한다. 제3도을 참조하면, 목록의 각 항목은 부분 이름 또는 기준(302) 및 그 부분 이름에 해당하는 정보 부분에 대한 보안 해시(301)를 포함한다. (예컨대, 파일에 기초한 군집화(file-based grouping)의 경우, 부분들의 목록은 모든 파일들의 파일 이름과 이에 해당하는 해시 결과를 포함하는 파일일 수 있다.)

목록은 이어서 DS(문서 서버, 100)에게만 알려진 비밀 키에 의해 디지털 서명된다. 문서에 디지털 서명하는 여러 가지 방법이 있다 (예컨대, [1] 참조). 그 한가지 방법은 부분들 목록의 MD5(또는 기타 보안 해시)를 계산하여 해시 결과를 비밀 키(208)를 사용하여 (서명을 하기 위해) 암호화하는 것이다. 부분들 목록과 서명이 함께 BOM(207)로 불리워진다. DS의 공개 키만이 BOM의 진정 여부(authenticity)를 조회하는데 필요하다는 점에 주목해야 한다.

암호 봉투의 진정 여부는 DS의 공개 키를 사용하여 서명을 해독하고, 그 결과를 부분들 목록의 MD5와 비교함으로써 검사된다. 둘이 서로 일치하면, 그 부분들 목록은 무단 변경되지 않았다. 개개의 부분들에 대한 진정 여부(authenticity)도 그 각 부분의 MD5를 계산하고 그 결과를 목록의 해당하는 항목과 비교함으로써 검사될 수 있다. 따라서, BOM(207)은 암호 봉투와 그 모든 부분들의 보존(integrity of a cryptographic envelope and all its parts)을 보장한다.

[암호 봉투는 일체완비됨(Cryptographic Envelope is Self-Contained)]

암호 봉투의 중요한 특징은 다음의 의미에서 일체완비(self-contained)된다는 점이다. DS의 공개 키만이 암호 봉투의 진정 여부를 조회하기 위하여 필요하다. 암호화된 PEK들(202, 210, 211, 제2도 참조)이 암호 봉투 내에 있으므로, BS의 비밀 키만이 내용을 복원하는데 필요하다. 더구나, 서로 다른 문서 서버(DS)들이 BS의 공개 키만을 사용하여 암호 봉투를 발생시킬 수 있으며, BS와 DS 사이에 기타의 통신이 필요치 않다.

[암호 봉투 작성 단계]

이제 암호 봉투의 작성을 위한 처리 단계들을 요약한다(제2도 참조).

1-a 암호 봉투 내에 포함도리 정보 부분들을 조립한다.

1-b 부분들에 선택적인 처리 단계들(예컨대, 압축, 사전 지문(pre-fingerprinting), 및 사전 워터마크(pre-watermarking)) 을 적용한다. 이 처리 단계들에 대한 충분한 상태 정보를, 나중에 이 작업들을 원상태로 되돌리기 위하여(undo the operations) 유지한다.

1-c 암호화될 각 부분에 대하여 하나씩 불규칙 PEK(random part encryption keys, 202)를 발생시킨다.

1-d 문서 부분들을 그들 각각의 PEK에 의해 암호화하여 암호화된 부분들(203, 204, 205)을 형성한다. 이 암호화된 부분들은 암호 봉투에 포함된다.

1-e 이어서, 이 PEK들이 BS의 공개 키를 사용하여 암호화되어 암호화된 PEK(202, 210, 211)를 형성한다. 이 암호화된 PEK들은 암호 봉투에 포함된다. 암호화된 PEK들과 이들에 해당하는 암호화된 부분들은 관련된다.

1-f 단계 1-b로부터의 명령들과 기타 상태 정보를 소정의 불규칙 PEK들을 사용하여 또한 암호화된다. 이 PEK들은 BS의 공개 키에 의해 암호화된다. 암호화된 부분들(203, 204, 205)과 암호화된 PEK들(202, 210, 211) 모두는 암호 봉투내에 놓여진다.

1-g 맛보기 부분(teasers), 초록, 및 목차(201)와 같은 깨끗한 텍스트 부분들(clear text parts)을 암호 봉투에 포함시킨다.

1-h 지문과 워터마크 처리 명령(205)와 가격 행렬(206)과 같은 기간과 조건들을 포함시킨다. 임의의 부분들 또는 필요한 경우에는 그에 대한 소부분(sub-parts)들을 암호화한다(그리고 그들의 암호화된 PEK들을 포함시킨다). 앞에서와 같이, 암호화된 부분들을 그들의 암호화된 PEK들과 관련시킨다.

1-i 정보 부분들의 목록(209)를 작성하여, 조립된 모든 부분들을 나열하고 목록의 각 부분들에 대한 보안 해시를 계산한다.

1-j 예컨대, 목록의 보안 해시를 계산하여 이를 DS 비밀 키에 의해 암호화하는 것과 같이 목록에 디지털 서명함으로써 BOM(207)에 대한 서명(208)을 작성한다. BOM(207) (목록(209)와 서명(208))은 암호 봉투에 추가된다.

가능한 암호 봉투 구조에 대한 상세한 사항은 제2도를 참조하면 된다.

[단계2 : 암호 봉투 배포]

암호 봉투가 작성되면, 예컨대 인터넷 상으로 전송하거나, 라디오 또는 텔레비전 신호, 케이블, 위성, CD-ROM, 및 BBS로 보내는 것과 같은 임의의 방법으로 배포될 수 있다. 이 배포에는 보안 유지가 필요하지 않다. 암호 봉투는 복사 및 복제될 수 있으며 사용자들 사이에서 공유될 수 있다. 사실상, 암호 봉투의 다운스트

링(down-stream) 배포(예컨대, 친구들에 의한 암호 봉투의 복사)가 암호 봉투를 배포하는 경제적인 방법이라고 예상하고 있다. 결국, 암호 봉투는 서버에 어떠한 보안 상의 요구사항을 부과하지 않고서도 임의의 서버에 저장될 수 있다.

[단계3 : 사용자에 의한 구매 요청]

이 단계는 종종 사용자가 보토의 텍스트(plain text)인 암호 봉투의 맛보기 부분(teaser, 201)을 훑어본(browsing) 후에 이루어진다. 암호 봉투 내용에 흥미가 있는 사용자는 BS로부터 필요한 PEK들을 구입하여야 할 것이다(제1도 참조).

[그래픽 사용자 인터페이스(Graphical User Interface)]

암호 봉투 구조를 반영한 수정된 웹 브라우저(web browser)와 같은 GUI의 도움을 받아 봉투를 훑어 본다. 먼저, 수정된 브라우저는 암호 봉투의 보존(integrity)을 검사할 수 있어야 한다. 사용자는 이 보존 검사를 통하여 암호 봉투에 대한 어떠한 무단 변경이라도 이를 보고 받는다. 다음으로, 브라우저는 예컨대, 초록과 목차를 표시하는 것과 같이 암호 봉투 내의 깨끗한 텍스트(clear texts)를 표시할 수 있어야 한다. 마지막으로, 제2도 및 제5도를 참조하면, 브라우저는 암호 봉투 (200)으로부터 필요한 부분들을 추출하여 BRM(Buy Request Message, 500)을 구성 할 수 있어야 한다.

[사전 등록(Prior Registration)]

BS가 사용자를 인식할 수 있도록 하기 위해 사용자가 사전 등록 단계를 수행한다고 가정한다. 예를 들어, 사용자는 신용있는 제3자에게 등록할 수 있다.

예컨대, 이 등록은 사용자에게 계좌 번호를 발행하는 등록 센터로 사용자가 전화하는 것을 수반할 수 있다. 이어서 그계좌 번호가 모든 BS들에 전송된다. 선택적으로, 등록 센터는 계좌 번호에 디지탈 서명을 할 수 있는데, 이 경우에는 BS에서 갱신할 필요가 없다. BS는 서명을 검사함으로써 계좌 번호를 조회하기만 할 수 있다.

등록 이후, 사용자에게 소정의 신임장(credentials) (예컨대, 계좌 번호와 기타의 회원 정보)이 발행된다. 신임장은 신용있는 제3자에 의해 디지털 서명된 문서로서, 이를테면 계좌 번호, 입회 관계(affiliations), 또는 사용자의 권리와 같은 정보를 포함하며, 또한 예를 들어 이 제3자는 사용자가 목록 가격에서 할인받을 수 있도록 해주는 소정의 북 클럽(book club) 회원 신임장을 사용자에게 발행할 수 있다.

[보안 DFWM(secure DFWM)]

본 발명의 방법의 보다 특수한 점은 등록의 결과 보안 DFWM(103, 제1도) (해독 지문과 워터마크 처리 모듈, decryption fingerprintion watermarking module)이 UPC에서 구체화(instantiate)된다는 점이다.

DFWM은 부분들을 해독함과 동시에 해독된 부분들에 지문과 워터마크 처리를 적용하는 역할을 한다. 워터마크 처리는 지우기 어렵지만 문서를 읽는 데에는 영향을 미치지 않게 문서 내에 볼 수 있는 표시를 한다. 지문은 문서 내의 보이지 않는 표시이며 따라서 제거하기 어렵다.

지문과 워터마크 처리 기법에 관한 상세한 정보는 1995년 6월 23일 출원된 미국 특허 제08/494, 615호를 참조하면 된다.

[DFWM의 구체화(Instantiation of DFWM)]

보안 DFWM을 여러 가지로 구현할 수 있다. 가장 간단한 방법은 공개 키 기법에 기초한 것으로, DFWM이 보안 유지 하에 비밀 키를 발생시켜 DFWM 보안경계 내에 저장한다. 예를 들어, DFWM은 의사 불규칙 수 발생기(pseudo-random number generator)를 사용하여 공용-비밀 키 쌍을 만들 수 있다. DFWM 비밀 키는 DFWM 내에 저장되며, 공개 키는 외부에 알려진다. 등록 과정은 신용있는 제3자가 DFWM 공개 키를 증명할 수 있도록 해준다 (공개 키 증명 과정(public key certification process)에 대해서는 예컨대 [1] 참조). DFWM 비밀 키는 DFWM 모듈이 가지는 유일한 비밀 정보이다.

[DFWM의 보안(Security of DFWM)]

DFWM은 물리적으로 보안이 유지되는 모듈(예컨대, 스마트 카드(smart cards)에서 동작하거나, (보안이 유지되지 않는) UPC 환경에서 동작하는 소프트웨어의 일부일 수 있다. 전자의 경우, 보안은 물리적인 무단 변경 방지 포장(physical tamper resistance of the packaging)을 통해 이루어진다. 현재의 포장 기술은 모든 실용적인 목적을 위한 DFWM에 충분한 보안을 제공할 수 있다.

본 명세서에서는 DFWM의 물리적인 보안을 가정하지 않은 후자의 경우에 초점을 맞춘다. 이 경우가 보다 흥미로운, 그 이유는 물리적인 보안이 가능하다면 그만큼 DFWM의 보안이 더 향상되는 것일 따름이기 때문이다.

보안이 유지되는 하드웨어가 없는 경우, DFWM의 보안은 보장되지 못한다. 실제의 여러 경우에, 공지의 소프트웨어 기법(예컨대, 바이러스 작성자에게 잘 알려진 코드 모호화 기법(code-obscuring techniques)을 사용하여 충분한 보안을 이룰 수 있다.

그러나, 본 명세서에서 기술하는 처리의 중요한 장점 중의 하나는,DFWM이 손상되더라도, 그 노출은 제한된다는 점이다. 사용자는 구입하지 않은 문서 부분을 열수는 없다 (이는 PEK를 가지고 있지 않기 때문이다). 구매 거래는 보안이 유지되는 BS를 통하여 이루어져야 하므로 그 보안이 유지된다.

DFWM이 손상되면 (즉, DFWM 비밀 키가 노출되면), 가능한 유일한 손실은 사용자가 구입한 문서가 정당하게 지문되고 워터마크되지 않았다는 것이다. 그러나, 보안 상의 위험은 사용자가 문서로부터 표시를 제거할 가능성과 완전히 상이한 것은 아니다.

[구매 요청 거래(Buy Request Transaction)]

이제 구매 요청 거래를 상세히 설명한다.

그래픽 사용자 인터페이스(GUI)를 통하여, 암호 봉투에 포함된 품목들의 목록이 사용자에게 표시된다. 사용자는 정보를 더 얻기 위하여 관련된 초록들을 훑어 볼 수 있다. 사용자는 또한 그 품목들의 목록 가격을 알 수 있다. 사용자가 그 품목들을 구입하고자 하는 경우, GUI를 통하여 구매 요청을 발하며, 그 결과 BRM(Buy Request Message) (500 참조, 제5도)이 BS(102)로 보내진다.

[사용자 인증(User Authentication)]

구매 요청이 완료되기 전에, 시스템은 사용자를 확인하고자 할 수 있다. 시스템이 사용자를 확인하는 기법으로는 공지된 여러 방법들이 있다. 예를 들어,(Pretty Good Privacy [3]에서 사용되는 것과 유사한) 이러한 기법의 하나로서 UPC의 디스크 드라이브에 암호화된 사용자 개인 키(user private key)를 저장하는 것이 있다.

사용자에게 그의 비밀 암호(password)를 요청하는 표시를 하는데, 비밀 암호는 개인 키를 해독하는데 사용된다. 개인 키는 디지털 서명을 하거나 구매 관련 메시지를 증명하는데 사용되며, 각 단계의 종료시에 소거된다.

[환경 변수(Environmental variables)]

환경 변수는 사용자 환경에 관한 정보 또는 UPC에 대한 정보 (예컨대, 장소, 시간, 기계형식, 운영체제이름, 등) 이다. 반면에, 사용자 신임장(user credentials)은 사용자에 관한 정보이다.

환경 변수는 보안형(secure)과 비보안형(insecure)의 두 가지 유형이 있다. 보안형 변수들은 조회되며 디지털 서명된다. 이들은 BS에 의해 (등록 중에) 검사되어 서명되거나 DFWM에의해 발생되어 서명될 수 있다.

비보안형 변수들은UPC에 의해 발생된다. 이들은 조회되거나 서명되지 않는다. 이들은 정보 목적으로만 포함된다. 본 명세서에 걸쳐서 환경 변수는 상기 두가지 유형을 모두 의미한다.

[구매 요청 메시지(Buy Request Message)]

제5도를 참조하면, BRM(500)은 암호 봉투로부터 복사되거나 추출된 다음의 정보를 포함한다(200, 제2도).

3.1 암호 봉투(207)의 BOM

3.2 구입할 품목들의 목록(list articles) (501)

3.3 품목들의 목록과 관련된 PEK 및 기타 제어 부분들(202 및 211)

3.4 (가격 행렬 등과 같은) 기간과 조건(206)

또한 BRM(500)은 사용자 환경, DFWM,또는 사용자로부터 복사되거나 추출된 다음의 정보를 포함한다.

3.5 사용자 신임장 목록(예컨대, 회원 및 할인 카드) 과 사용자 인증 관련 정보 (502)

3.6 사용자 신임장 목록 (예컨대, 날짜 및 시간, 장소,DFWM 또는 기계 하드웨어 ID) (503)

3.7 DFWM 공개 키(504)

암호 및 인증과 같은 표준 암호 기법들이 BRM에 적용될 수 있다. BRM의 인증을 위한 한가지 방법은 BRM 전체의 MD5를 계산하고, DFWM의 비밀 키를 사용하여 MD5 결과를 암호화하므로써 서명(505)를 발생시키는 것인데, 이 서명(505)은 BRM의 종단에 추가 된다.

이제, BRM의 발생에 앞서는 단계들을 요약한다.

3-a GUI를 통하여 암호 봉투의 깨끗한 텍스트로 된 부분들을 읽는다.

3-b 구입할 암호 봉투의 정보 부분들을 선택

3-c 구입의 기간과 조건(206) (예컨대, 목록 가격, 재배포하지 않는다는 약정) 에 대한 사용자의 명시적인 동의

3-d 인증을 위하여 사용자로 하여금 비밀 암호를 입력하도록 표시. (그결과 소정의 사용자 인증 관련 정보가 발생되며 BRM에 포함된다.)

3-e GUI 의한 BRM(500)의 발생

3-f BRM을 BS로 전송

주 :BRM은 암호 봉투의 특수한 형태 (즉, 구매요청 암호 봉투)로 볼 수 있다.

[단계 4 :구매 서버 응답(Buy Server Response)]

BRM을 수신함과 더불어 BSR(Buy Server Response)가 전송된다. 이제, BSR의 전송 이전에 BS(구매 서버)가 행하는 동작을 자세히 설명한다.

[사용자 계좌 (User Account)]

BS 가 BRM을 수신하면, BOM을 조회하여 제어 부분들의 진정 여부를 검사한다.

BS는 DFWM 공개 키의 진정 여부, 사용자 신임장, 및 사용자 인증 관련 정보를 또한 검사한다. 사용자는 사전의 등록 단계에서 BS에 계좌를 가지고 있을 수 있으며, 이 경우, (사용자가 받을 수 있는 소정의 할인을 적용한 후) 적절한 금액이 사용자 계좌로부터 청구된다.

[기간과 조건의 평가(Evaluation of Terms and Conditions)]

암호 봉투에 포함된 (BRM에도 또한 포함된) 기간과 조건(206)의 주된 목적은 사용자가 구입을 완료하는데 필요한 기간과 조건이 기개된 요구사항들을 충족시키는 것을 보장하는 것이다. BS는 이 기간과 조건을 평가(실행)함으로써 사용자가 요구사항들을 만족시키는지 검사한다. 평가 결과에 의해 구입이 완료될 수 있는지가 결정된다. 그 결과 가 긍정이라면, 다음 단계들이 계속되며, 그렇지 않은 경우에는 에러 메시지가 BSR에 포함된다. 결과가 긍정인 경우, 실제 구입 가격은 또한 가격 행렬(400)에 주어진 공식 (401)을 사용하여 계산된다.

[키 번역(Key Translation)]

BS가 BRM에 대하여 수행하는 동작 중의 하나로서 키 번역이 있다. 단계 1에서 언급한 바와 같이, PEK(부분 암호화 키)들은 BS 의 공개 키를 사용하여 암호화된다. BS는 그 비밀 키를 사용하여 암호와된 PEK들을 해독한다. 암호화된 PEK를 해독한 후,BS는 그 PEK들을 DFWM의 공개 키를 사용하여 다시 암호화하여 DFWM만이 PEK를 복원할 수 있도록 한다. 이것이 키 번역 단계이다.

[커스텀화된 지문과 워터마크 처리(Customized Fingerprinting and Watermarking)]

BS가 수행하는 다른 부류의 동작으로서 지문과 워터마크 처리 명령의 커스텀화가 있다. 단계 1에서 언급한 바와 같이, 이들 명령은 BS 공개 키를 사용하여 암호화되며 제어 부분으로서 암호 봉투에 실린다. BS는 먼저 이 명령들을 해독하고, 이어서 명령 안에 사용자에 관한 정보 (예컨대, 사용자 이름, 회원 번호) 와 처리에 관한 정보 (예컨대, 구입 날짜, 라이센스 제한, 처리 ID)를 포함시킨다. 이 명령들은 이어서 DFWM 공개 키를 사용하여 암호화된다. (DFWM은 문서를 해독하기 전에 이들 암호화된 지문과 워터마크 처리 명령들이 존재하는지를 검사한다.)

[기간과 조건의 변환(Transformation of Terms and Conditions)]

내용을 사용하는데 대한 제한에 관계되는 기타의 사항들이 BSR에 포함된다. BRM에 포함된 기간과 조건은 강화되거나 수정될 수 있다(예컨대, 암호 봉투가 생성되었기 때문에 기간이 변경되었을 수 있다). 결과적인 기간과 조건은 문서 사용에 관한 제한, 기간과 조건을 언급하는 소정의 간단한 보통 텍스트(plain text)일 수 있다. 또한, 이들은 기간과 조건을 강제시키는 실행가능한 명령, 객체, 및 에이전트(agents)일 수 있다.

[구매 응답 단계(Buy Response Steps)]

제6도를 참조하면, BS에 의해 행해지는 단계들을 BRM을 수신하는 단계로부터 BSR을 전송하는 단계까지 요약하기로 한다.

4-a BRM을 수신

4-b (BOM을 검사함으로써) BRM의 진정 여부 검사, 사용자 신임장 조회, 사용자 인증 관련 정보 조회, DFWM 공개 키 조회, 환경 변수 검사

4-c (BRM으로부터의) 사용자 신임장, 가격 행렬 및 환경 변수를 그리고 (BS로부터의) 데이터 베이스의 사용자 정보와 부가적인 환경 변수들을 입력으로서 사용하여 기간과 조건을 평가. 기간과 조건 평가의 출력은 (a) 사용자가 부분들에 접속하도록 허용할 것인지와 (b) 부분들을 구입하기 위한 실제 가격(601)이다.

4-d 사용자가 접속하도록 허용되는지와 사용자가 충분한 신용을 가지는지를 검사한다. 그렇지 않은 경우, 중단(abort)하고 에러 BSR을 전송한다.

4-e PEK들을 번역한다. (BS 개인 키를 사용하여 PEK를 해독하고 DFWM 공개 키를 사용하여 PEK를 재암호화한다.) 번역된 PEK들(602, 603)을 BSR에 포함시킨다.

4-f 지문과 워터마크 처리 명령들을 커스텀화한다. (명령들을 해독하고, 사용자의 특정 정보와 거래 관련 정보를 명령들에 포함시킨다. DFWM 공개 키를 사용하여 수정된 명령들을 암호화한다.) 이들을 BSR(604)에 포함시킨다.

4-g 변환된 기간과 조건 및 문서의 사용 상의 기타 제약들을 BSR에 포함시킨다(605).

4-h BSR을 사용자에게 보낸다.

BSR은 암호 봉투의 특수한 형태, 즉 라이센스 암호 봉투(License Cryptographic Envelope)로서 생각될 수 있다. 암호화 및 인증과 같은 표준 암호기법들이 사생활(privacy)과 BSR(606)의 진정성(authenticity)을 보호하기 위해 채용 될 수 있다.(예컨대, [1] 참조.)

[단계5 : 암호 봉투의 개봉(Opening of Cryptographic Envelope)]

이것이 마지막 단계이다. 이 단계를 위한 사전 조건은 BSR을 BS로부터 수신하는 것이다. BSR을 수신한 후에, 사용자는 편리할 때로 암호 봉투를 열 수 있다.

BSR은 암호 봉투의 잠금을 푸는 키(key)이다. PEK들이 모두 DFWM 공개 키로 암호화되었으므로, BSR의 내용은 그 특정 DFWM만 사용가능하다. 제6도을 참조하면, 암호 봉투를 개봉하는데 관계되는 단계들은 다음과 같다.

5-a DFWM은 BSR(606)의 진정 여부를 보장하기 위하여 검사한다. 개봉절차는 BSR 인증이 성공적인 경우에만 계속된다.

5-b 사용자에게는 BSR의 갱신된 라이센싱 기간과 조건(605)이 선택적으로 표시된다. 개봉 절차는 사용자가 이 기간과 조건에 동의하는 경우에만 계속된다.

5-c DFWM은 번역된 PEK(602, 603)와 커스텀화된 지문과 워터마크 처리명령(604)의 진정 여부를 확인하며 이를 해독한다. 개봉 절차는 이 인증이 성공적인 경우에만 계속된다.

5-d 해독된 PEK를 사용하여, DFWM은 암호 봉투(203, 205)의 해당하는 암호화된 부분들을 해독한다.

5-e DFWM은 해독된 문서에 적절한 지문과 워터마크 처리 명령(604)를 적용한다. (지문과 워터마크는 사용자에게 커스텀화되며, 무단의 배포에 대하여 추가적인 방지를 해준다.)

5-f 해독된 문서 결과는 DFWM 보안 구역 외의 사용자에게 배포된다.

발명의 효과

암호 봉투 처리는 (환자 의료 기록과 같은) 매우 민감한 데이터나 데이터 베이스의 효율적이고, 보안 유지가 되며, 분산되어 있는 제어를 구현하는데에도 일반적으로 사용될 수 있다.

본 발명에 따르면, 문서 서버와 구매 서버 사이의 신뢰관계를 보다 명백히 분리할 수 있게 된다. 따라서, 허가된 사용자만이 보안 정보 부분의 깨끗한 텍스트 내용에 접근할 수 있으며, 임의의 수의 사용자에게 임의로 배포될 수 있는 암호 봉투의 작성 방법이 제공된다.

[참조 문헌]

1. 비. 쉬나이어(B. Schneier) 저, 응용 암호학(Applied Cryptography), 제2판 애디슨 웨스리(Addison Wesley) 출판사, 1996.

2. IBM CD 쇼케이스(CD-Showcase) 특허 (미합중국 특허 제5,319,705호).

3. 에스. 가핑켈(S. Garfinkel) 저, 프리티 굿 프라이버시(Pretty Good Privacy), 오레일리 앤드 어소시에이트사(O'Reilly Associates, Inc), 1994.

4. 엘. 더블유. 월(L. W. Wall)과 알. 엘. 슈바르쯔(R. L. Schwartz) 저, 펄 프로그래밍(Programming Perl), 오레일리 앤드 어소시에이트 사, 1991.

5. 비. 콕스(B. Cox) 저, 슈퍼디스트리뷰션과 전자 객체(Superdistribution and Electronic Objects), 도브 박사 저널(Dr. Dobb's Journal), 제17권, 제10호, 1992년 10월.

6. 발명의 명칭이 개별화를 통하여 문서 및 지적 재산권 프라이버시를 보호하기 위한 방법(A Method to Deter Document and Intellectual Property Privacy Through Individualization)인 1995년 6월 23일자 미합중국 특허 출원 제08/494,615호.

(57) 청구의 범위

청구항 1. 복수의 사용자에게 임의로 배포될 수 있는 암호 봉투 - 상기 봉투는 정보 부분들의 집단인 디지털 문서이다 - 를 작성하는 방법에 있어서, a. 암호화된 부분 - 상기 부분은 상기 봉투에 포함된다 - 을 생성하기 위하여 부분 암호화 키에 의해 상기 정보 부분들 중의 하나를 암호화하는 단계, b. 암호화된 부분 암호화 키 - 상기 암호화된 부분 암호화 키는 상기 봉투에 포함된다 -를 생성하기 위하여 제1 공개 키에 의해 상기 부분 암호화 키를 암호화하는 단계, c. 상기 봉투에 포함되는 부분들의 목록 - 상기 목록의 각 항목은 부분 이름과 상기 이름을 가진 부분의 보안 해시를 포함하며 상기 목록도 상기 봉투에 포함된다 - 을 작성하는 단계, 및, d. 서명 - 상기 서명은 상기 봉투에 포함된다 -을 생성하기 위해 제1 비밀 키에 의해 상기 목록에 서명하는 단계, 를 포함하며, 상기 목록의 보존은 상기 제1 비밀 키와 관련된 제2 공개 키를 사용하여 상기 서명을 조회함으로써 검사될 수 있으며, 상기 봉투의 임의의 한 부분의 보존은 상기 한 부분의 제2 보안 해시를 계산하고 상기 제2 해시를 상기 목록의 그에 해당하는 해시와 비교함으로써 검사될 수 있으며, 상기 암호화된 부분의 정보내용은 공개가 방지되고 상기 부분 암호화 키에 의해서만 복원될 수 있으며, 상기 부분 암호와 키는 상기 제1 공개 키에 해당하는 제2 비밀 키를 사용하여 상기 암호화된 부분 암호화 키를 해독함으로써 복원되는 암호 봉투 작성 방법.

청구항 2. 제1항에 있어서, 상기 문서의 상기 부분들 중의 선택된 부분들을 삽입, 삭제 또는 상기 선택된 부분들의 선택된 워드 또는 비트들의 변경에 의하여 수정하고, 각각의 수정되지 않은 문서를 복원하기 위하여 각각의 수정된 문서 부분과 관련된 상태 정보를 그 수정과 함께 유지하는 단계를 더 포함하는 암호 봉투 작성 방법.

청구항 3. 제2항에 있어서, 상기 수정은 상기 부분의 상기 암호화 이전에 상기 부분들의 상기 선택된 부분들에 대하여 행해지며, 상기 상태 정보는 제3 부분 암호화 키 - 상기 제3 부분 암호화 키는 제3 공개 키에 의해 암호화된다 -를 사용하여 암호화되는 암호 봉투 작성 방법.

청구항 4. 제1항에 있어서, 상기 암호 봉투는 서버에서 실행될 컴퓨터 프로그램을 포함하여, 상기 실행의 결과는 상기 서버에 의한 후속 동작을 결정하는 암호 봉투 작성 방법.

청구항 5. 제4항에 있어서, 상기 프로그램은 상기 암호 봉투 내의 상기 정보 부분들의 접속에 대한 기간과 조건을 기술하며, 상기 실행은 상기 정보 부분들로의 접속을 허용할 것인지의 여부를 결정하는 암호 봉투 작성 방법.

청구항 6. 제4항에 있어서, 상기 프로그램은 각 문서 부분을 수정하기 위한 명령들을 포함하며, 각각의 부분은 삽입, 삭제, 또는 각 부분의 선택된 워드 또는 비트들의 변경에 의해 수정되며, 각각의 수정되지 않은 문서를 복원하기 위하여 각각의 수정된 문서 부분에 관련된 상태 정보를 그 수정과 함께 유지하는 암호 봉투 작성 방법.

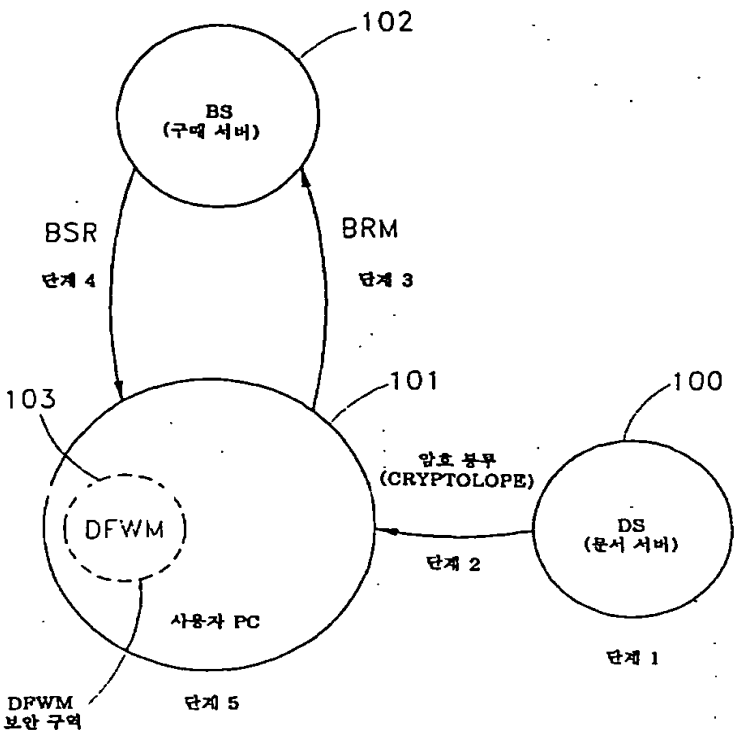
청구항 7. 암호 봉투의 내용 데이터로의 접속을 제공하는 방법에 있어서, a. 사용자로부터 서버로 요청을 전송하는 단계 - 상기 요청은 상기 암호 봉투의 부분에 접속하기 위한 요청이며, 상기 요청은 상기 부분을 암호화하는데 사용된 키를 공개 키로 암호화한 암호화된 부분 암호화 키를 적어도 포함한다 - 와, b. 상기 요청에 응답하여, 상기 서버로부터 상기 사용자로 응답을 전송하는 단계 - 상기 응답은 상기 암호화된 부분 암호화 키를 변환한 것이다 - 를 포함하며, 상기 변환은, 상기 공개 키에 관련된 비밀 키를 사용하여 상기 암호화된 부분 암호화 키를 해독하는 단계, 제2 공개 키를 사용하여 상기 부분 암호화 키를 암호화하는 단계, 상기 비밀 키를 사용하여 상기 변환된 키를 상기 부분 암호화 키로 해독하는 단계 - 상기 선택된 부분은 상기 부분 암호화 키를 사용하여 깨끗한 텍스트로 해독되어 상기 사용자에게 접속을 제공한다 -, 에 의하여 발생되는 접속 제공 방법.

청구항 8. 복수의 단말기로 전자 접속할 수 있는 서버를 가지는 통신 망에서, 암호 봉투의 선택된 내용 데이터로의 접속을 허가하는 방법에 있어서, 상기 암호 봉투는, a. 복수의 사용자에게 임의로 배포될 수 있는 암호 봉투 - 상기 봉투는 정보 부분들의 집단인 디지털 문서이다 - 를 작성하는 단계로서, 상기 암호 봉투 작성 단계는, (i) 보호될 상기 부분들의 각각 - 상기 부분들 중의 하나는 상기 선택된 내용 데이터를 포함한다 - 에 대하여 부분 암호화 키를 관련시키는 단계, (ii) 상기 부분을 각각을 그와 관련된 부분 암호화 키에 의해 암호화하는 단계, (iii) 상기 부분 암호화 키 각각에 대한 암호화된 부분 암호화 키를 생성하기 위하여 공개 키에 의해 상기 부분 암호화 키 각각을 암호화하는 단계, (iv) 부분들의 목록 - 상기 목록의 각 항목은 상기 부분들의 하나에 대한 부분 이름과 상기 하나의 부분에 대한 보안 해시를 포함한다 - 을 작성하는 단계, 및, (v) 서명을 생성하기 위해 비밀 키에 의해 상기 목록에 서명하는 단계 - 상기 암호 봉투는 상기 서명, 상기 목록, 상기 암호화된 부분 암호화 키, 상기 암호화된 부분들, 및 상기 정보 부분들의 암호화되지 않은 부분들의 집단이다 -, 를 포함하는 암호 봉투 작성 단계, 및, b. 상기 암호 봉투의 사본을 가진 사용자가 상기 선택된 내용 데이터에 접속하려고 하는 경우, 상기 접속은, (i) 상기 사용자로부터 서버로 요청을 전송하는 단계 - 상기 요청은 상기 암호 봉투의 부분에 접속하기 위한 요청이며, 나중의 상기 부분은 상기 선택된 내용 데이터를 포함하며, 상기 요청은 나중의 상기 부분을 암호화하는데 사용된 암호화 키를 공개 키로 암호화한 암호화된 부분 암호화 키를 적어도 포함한다 - 와, (ii) 상기 요청에 응답하여, 상기 서버로부터 상기 사용자로 응답을 전송하는 단계 - 상기 응답은 상기 요청의 상기 암호화된 부분 암호화 키를 변환한 것을 포함한다 - 를 포함하며, 상기 변환은, 단계 b (i)의 상기 공개 키에 관련된 비밀 키를 사용하여 상기 암호화된 부분 암호화 키를 해독하는 단계, 제2 공개 키를 사용하여 상기 요청의 상기 부분 암호화 키를 암호화하며, 상기 제2 공개 키에 관련된 상기 비밀 키를 사용하여 상기 변환된 키를 상기 요청의 상기 부분 암호화 키로 해독하는 단계 - 상기 선택된 부분은 상기 요청의 상기 부분 암호화 키를 사용하여 보통의 텍스트로 해독되어 상기 사용자에게 접속을 제공한

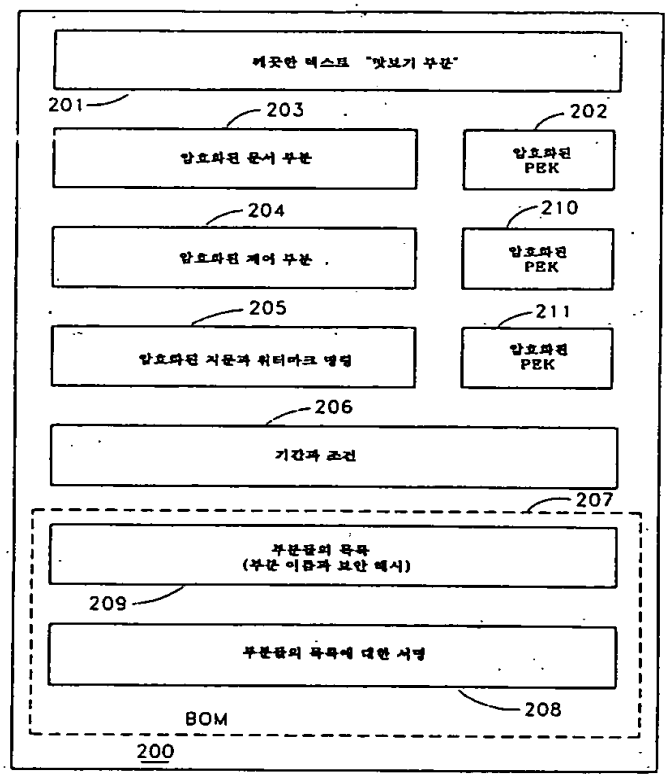
다 -, 에 의해 발생되는 [redacted] 제공 방법.

도면

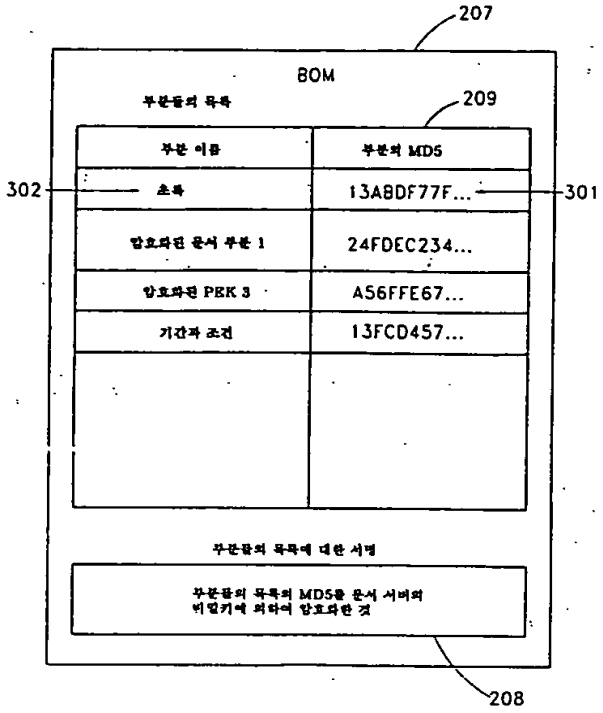
도면1



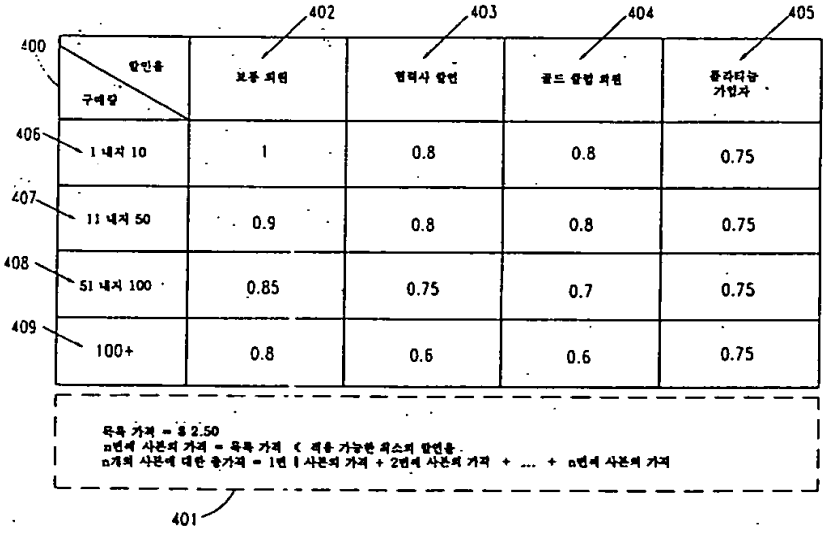
도면2



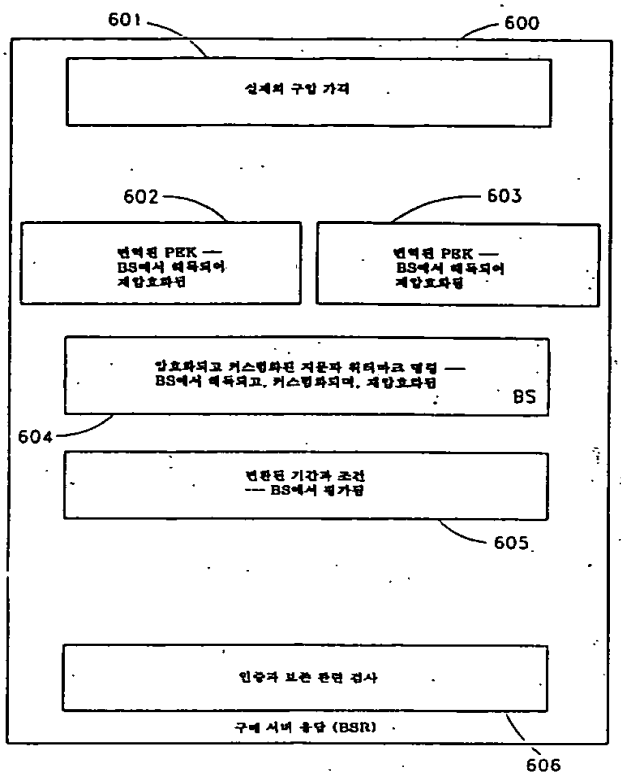
도면3


207
BOM
부품들의 목록
209
부품 이름
부품의 MD5
302
초록
13ABDF77F...
301
암호화된 문서 부분 1
24FDEC234...
암호화된 PEK 3
A56FFE67...
기간과 조건
13FCD457...
부품들의 목록에 대한 서명
부품들의 목록의 MD5을 문서 서버의
비밀키에 의하여 암호화한 것
208

도면4


400
402
403
404
405
할인율
구매량
보통 회원
법적사 할인
골드 할인 회원
플래티늄 가입자
406
1 내지 10
1
0.8
0.8
0.75
407
11 내지 50
0.9
0.8
0.8
0.75
408
51 내지 100
0.85
0.75
0.7
0.75
409
100+
0.8
0.6
0.6
0.75
목록 가격 = $ 2.50
n번째 사본의 가격 = 목록 가격 (적용 가능한 최소의 할인율 .
n개의 사본에 대한 총가격 = 1번 l 사본의 가격 + 2번째 사본의 가격 + ... + n번째 사본의 가격
401

도면5


601
600
실제의 구입 가격
602
603
변역된 PEK —
BS에서 획득되어
제압호화된
변역된 PBK —
BS에서 획득되어
제압호화됨
암호화되고 커스텀화된 지문자 워터마크 명칭 —
BS에서 획득되고, 커스텀화되며, 제압호화됨
BS
604
변환된 기간과 조건
— BS에서 제거됨
605
인증과 보존 콘텐 검사
구매 서버 응답 (BSR)
606